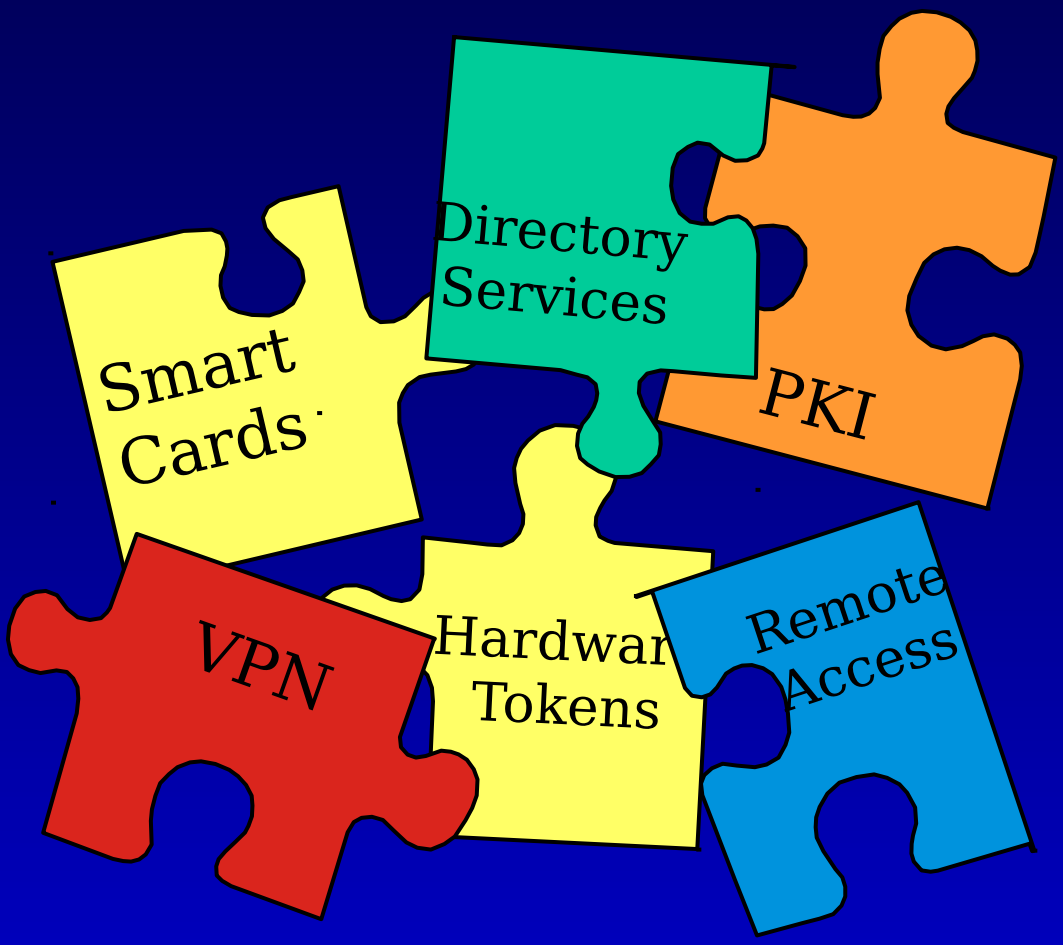
Public Key Infrastructure, Smart Cards, and Remote Access

Mr. Herman Karhoff
MITRE
28 June 2000

Original Tasking

- Educate the IMACS CMT on PKI and how it ties together the major technologies impacting the security of DoD networks and Interservice information



How does this affect the Interservice Community and

Agenda

- Background
- Definitions & Concepts
  - Public Key Infrastructure (PKI)
  - Smart Cards / Hardware Tokens
  - Remote Access/VPN
- Authentication and Authorization
- Technology Impacts
  - PKI
  - Hardware Tokens (e.g. SecurID)
  - Directory Services
- Challenges/Issues
- Summary
- Questions

Background...

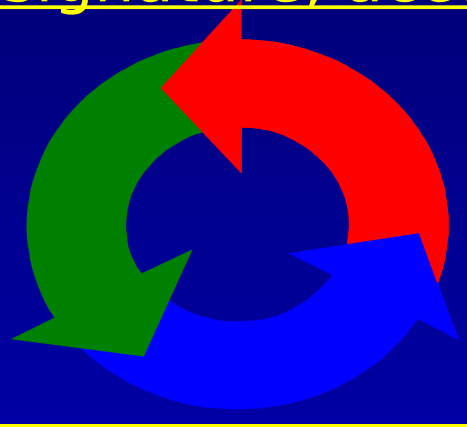
- DoD downward direction to deploy PKI was initiated in August 1997 (Money/Hamre letters)
- DoD X.509 Certificate Policy, Version2, March 1999
- Memo from Dr. Hamre dated 10 Nov 99
  - DoD will have a standard Smart Card called the Common Access Card (CAC)
    - Card will have an Integrated Circuit (IC) for storage of a PKI Private Key (details not yet specified)
    - May have barcode and/or magnetic swipe for building access
    - Will also act as primary military and civilian identification (photo?)
- New organization formed: Smart Card Configuration Management Control Board (SCCMCB) chaired by a Flag/SES appointed by Sec. Navy

PKI Definition

An electronic system of hardware, software, protocols, asymmetric keys, digital certificates, tokens, and a certificate management structure which in whole provides the infra-structure for the identification & authentication, data integrity, non-repudiation, digital signature, access control and confidentiality

Certificate Management

NSA & DISA

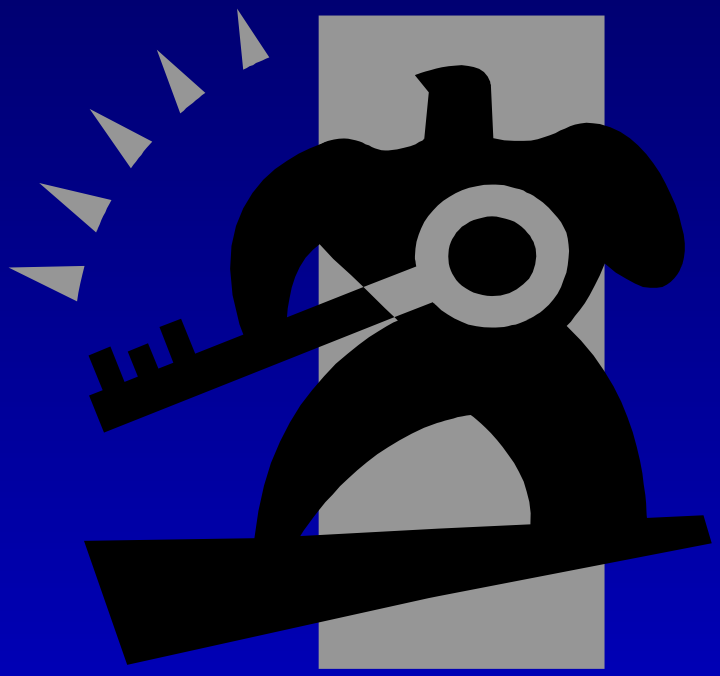


Registration Process

Services

PKI-Enabled Applications Users

Definition
Public Key Infrastructure (PKI)



The framework and services that provide for the generation, production, distribution, control, accounting and revocation of public key certificates.

Definitions: Public Key Infrastructure (concluded)

- Method of authentication and encryption using two keys - private and public

- Requires
  - Secure means of storing private keys
    - Floppy disk - level 3 PKI (not a secure solution)
    - Cryptographic Smart Cards - level 4 PKI (Not currently available for large-scale implementation)
  - A trusted method of finding others' public keys
    - Directory Services
    - Messaging Certificate (Trusted Third Party)

Definitions: Hardware Tokens

- One-Time Passwords
  - Require servers, but not readers
  - Challenge / Response
  - Time-Synchronous (e.g. SecurID)
- Smart Cards
  - Require readers
  - Cryptographic
  - Stored Value

Remote Access: Dial-in and VPN

- Remote Access users have higher authentication requirements than “desktop” users
  - Current dial-in system (RAS) requires only username and password (single authorization scheme)
  - VPNs, because they typically use the Internet for connectivity, require even higher authentication
- Hardware tokens increase security by adding an additional authorization scheme
  - Hardware tokens can be used with dial-in and VPNs

Who Will Use PKI In DoD?

"Eventually, nearly all DoD employees will likely need a PKI to support daily activities. The rest of the Federal Government and the Commercial Sector will likely use PKI services as well. These services are becoming increasing important in networked environments where communications and transactions occur over unsecure channels. Both the needs for confidentiality and integrity (including digital signature) can be provided by cryptography, and those cryptographic mechanisms need the support of a PKI."

How Will PKI Be Used In DoD?

- Identification and authentication for purposes of gaining access to computers and other resources (instead of passwords)
- Securing financial transactions
- Secure messaging with confidentiality and integrity of data transmitted
- Secure client-server transactions via the Secure Socket Layer (SSL) protocol

DoD Programs Identified to use PKI Services

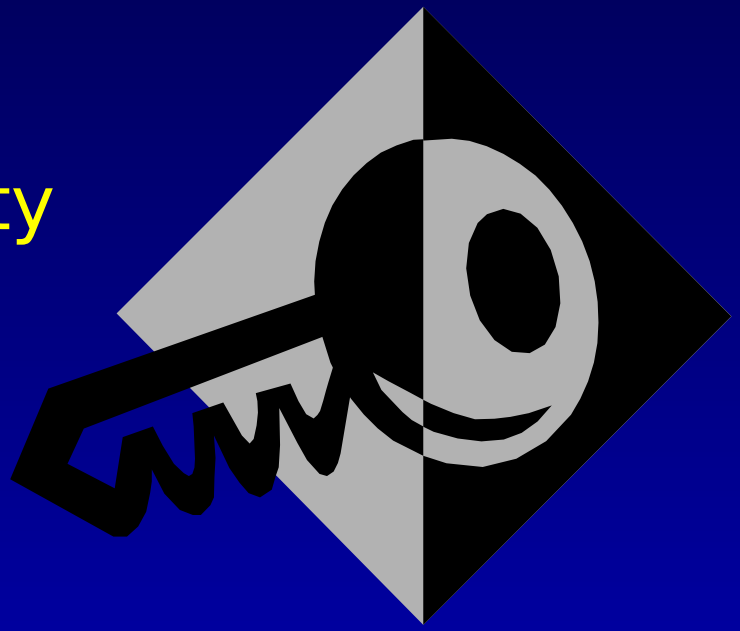
- Defense Messaging System (DMS) - the original driver for PKI services based on Multilevel Information Systems Security Initiative (MISSI) technology
- Global Command and Control System (GCCS) - access control to data and services used remotely
- Global Combat Support System (GCSS) - used PKI services to secure Web transactions
- Defense Travel System (DTS) - using digital signatures to approve travel of subordinates and sign electronic vouchers for travel expenses incurred
- Standard Procurement System (SPS) - to provide digital signature and confidentiality for procurement documents and transactions

Authentication Schemes

- Something you KNOW
  - Username / Password pair
- Something you HAVE
  - Hardware Token
- Something you ARE
  - Biometrics

What does PKI deliver?

- Proves author’s identity
- Ensures content integrity
- Provides message confidentiality



Definitions: Authentication and Authorization

- Authentication
  - Verification of a person's (or resource's) identity
- Authorization
  - Granting a user (or service) permission to perform an activity

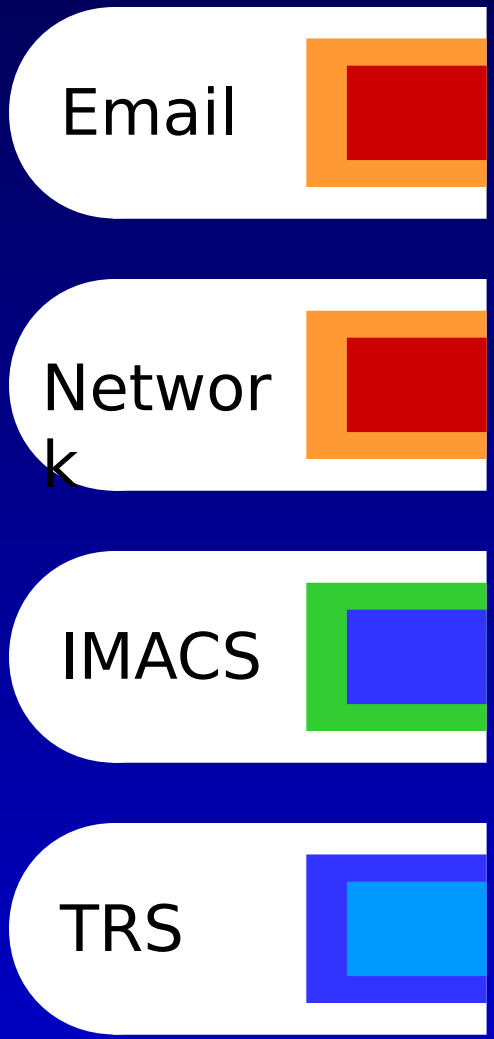
Relationship Between Authentication and Authorization

Step 1: User connects to an application and requests serv

Step 2: Authentication routine verifies User's identity

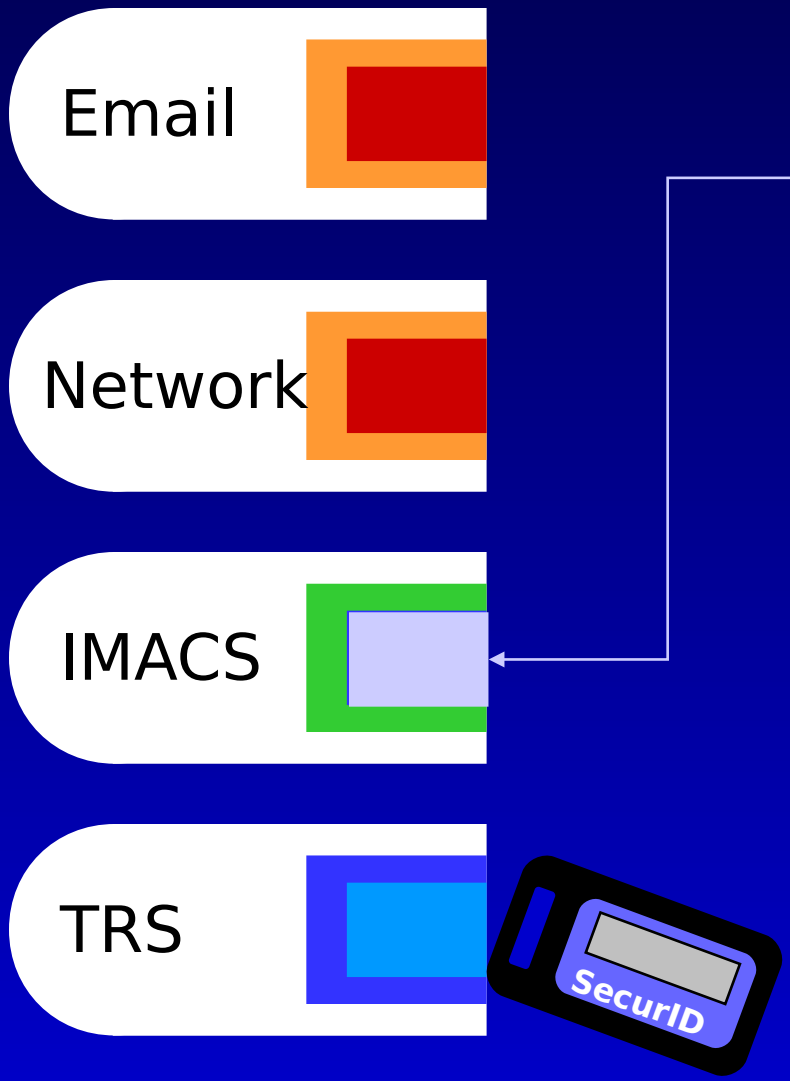
Step 3: Authorization routine determines User's privilege

Current Authentication and Authorization in AF & DoD Systems



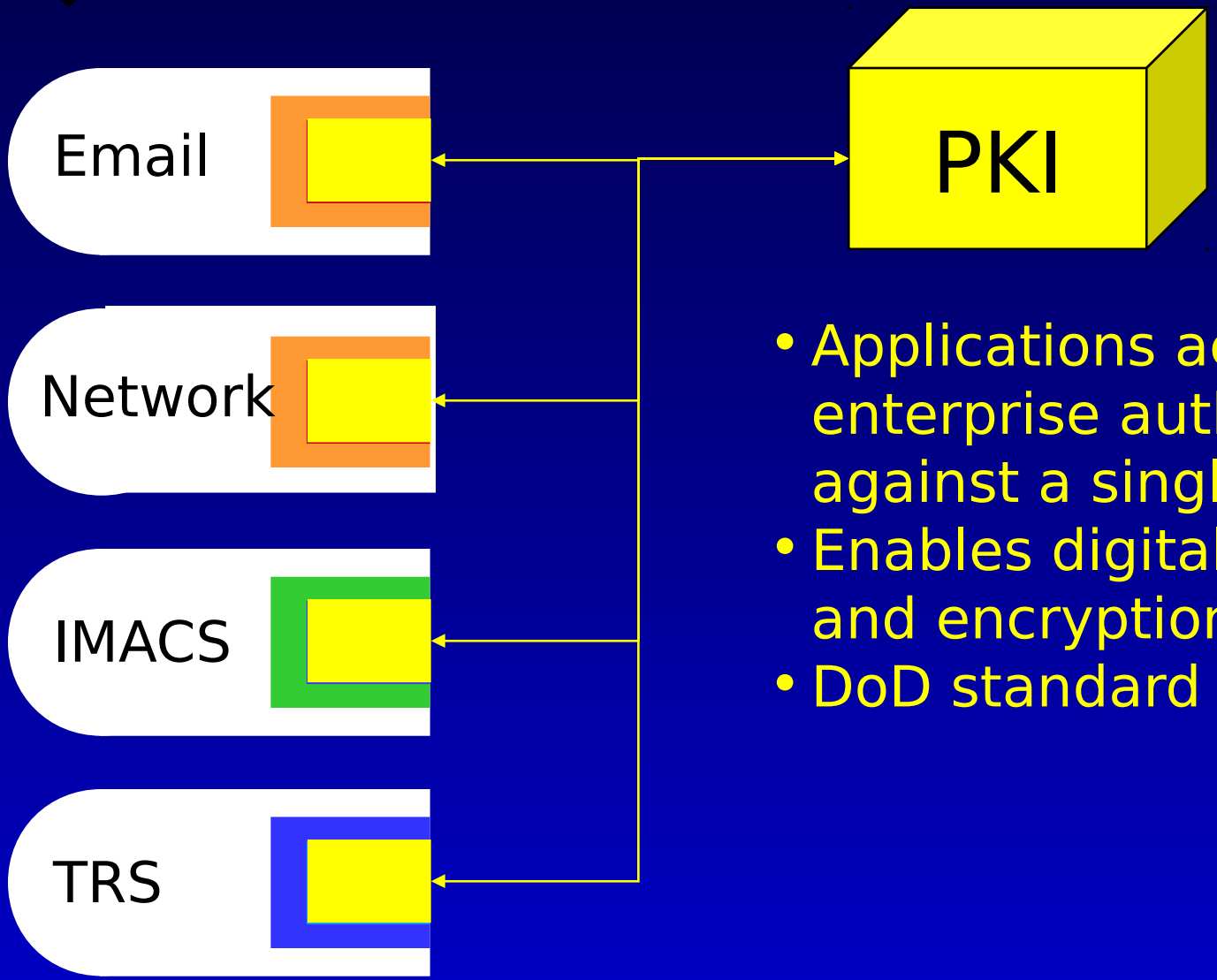
- Personal e-mail and network sign-ons share an integrated authentication and authorization scheme via NT domain
- Most applications use system-specific authentication and authorization
- An application typically uses a single authentication scheme (i.e., username and password)

Hardware Token Authentication



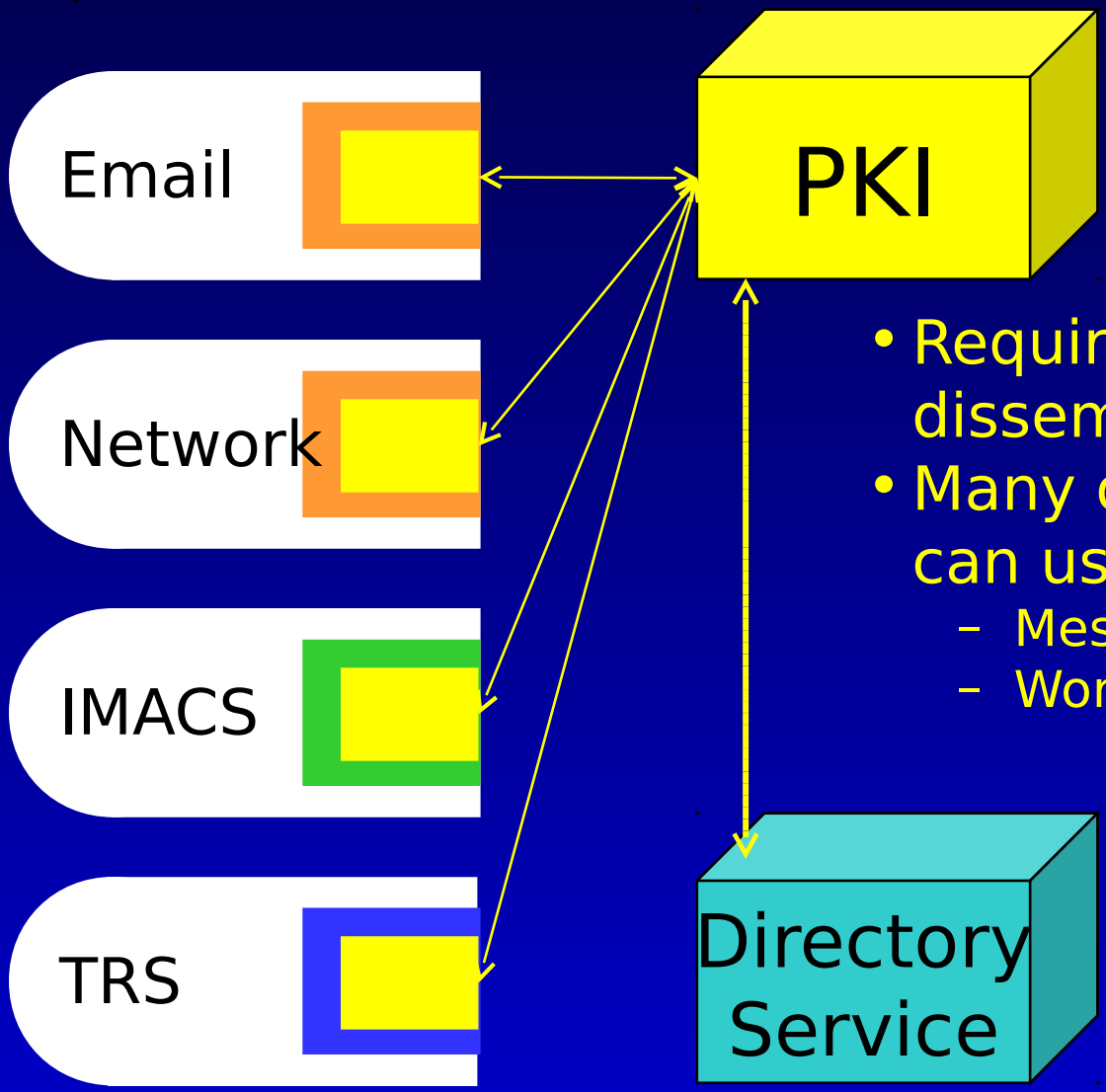
- Replaces authentication portion of its affiliated application(s)
- Significantly improves security by adding a second authentication scheme
- Issues
  - No digital signature
  - No encryption included
  - No standards defined

PKI Integration (Ideal World)



- Applications across the enterprise authenticate against a single entity
- Enables digital signature and encryption
- DoD standard is defined

Directory Services

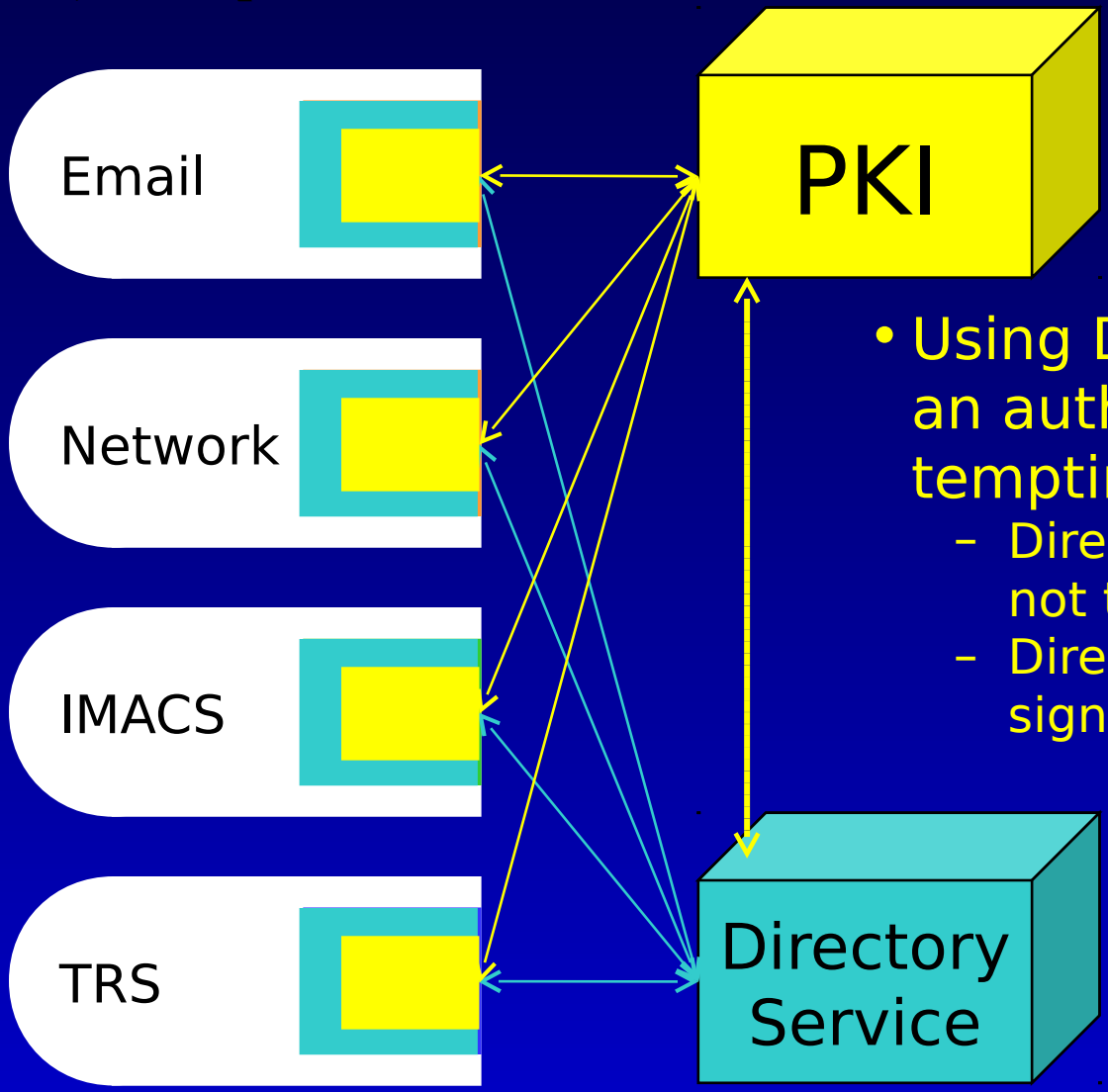


- Required by PKI for disseminating Public Keys
- Many other applications can use Directory Services
  - Messaging
  - Workflow

Why does PKI need Directory Services?

- Directory Services (DS) provide a way for users to quickly find Public Keys
- Directories are storage structures, designed for speed
- Directory Services have many possible applications outside of PKI

Directory Services (As an Authorization Source)



- Using Directory Services as an authorization tool is tempting, but...
  - Directory synchronization is not timely
  - Directory Server becomes a significant security risk

PKI Pre-Requisites

- Processes
- Certifying Authority
- Key Generation
- Private Key Storage
  - Smart card
- Public Key Dissemination
  - Directory Services
- Certificate Revocation List (CRL) Dissemination

Definition - Key Pair

- Private Key
  - Held by an *individual* entity
    - Typically a user, but may be a server
  - **Never** revealed, copied or transmitted
- Public Key
  - Designed for *others* to use for authenticating the holder of its corresponding Private Key
  - Copied and transmitted, in a controlled manner, as needed

Key Pair Generation

Two very large, mathematically-related numbers

- Data encrypted with one of the keys can only be decrypted with the other
- The Public Key is derived from the Private Key, but it is mathematically unfeasible to derive the Private Key from the Public Key

What does a Private Key look like?

```
-----BEGIN KEY MESSAGE-----
1QEAAy6AuD4AAAECA0ymCkXVB3fm3893hhdFDaAQQpnNMOo234Iop+23
Po9I8u0JttYY6/rdSDW5+HHfaqweYDS645G6+MJPHSD39FJJO3KuKFSD
PPrSWMZnxIhHHGD4M2S0A00jDHFMlPP23INMMN2N90JJKju//SDF+Hio
PnIO+23JFNLPAnn3342MN9U7ggg6DFER/234NBnntT54oo921+T8SDDM
BniGn9Au86P2A+INNKww34mER1iNjj2309+KlWWIUb623/2/VtQLKmii
=XFpM
------END OF KEY-----
```

What is a Public Key Certificate?

- An electronic record containing…
  - A person's name*
  - That person's Public Key
  - Date the certificate was issued
  - Date the certificate expires
  - A serial number
  - Possible other information, but information subject to change (e.g. rank, organization) should **not** be included
- Standard for PKI certificate format - X.509
- In a typical PKI environment, this record is signed using the Certifying Authority's Private Key

* Servers and other entities can have certificates. In this case, the entity's name would take the place of the person's name.

Definition
Certifying Authority (CA)

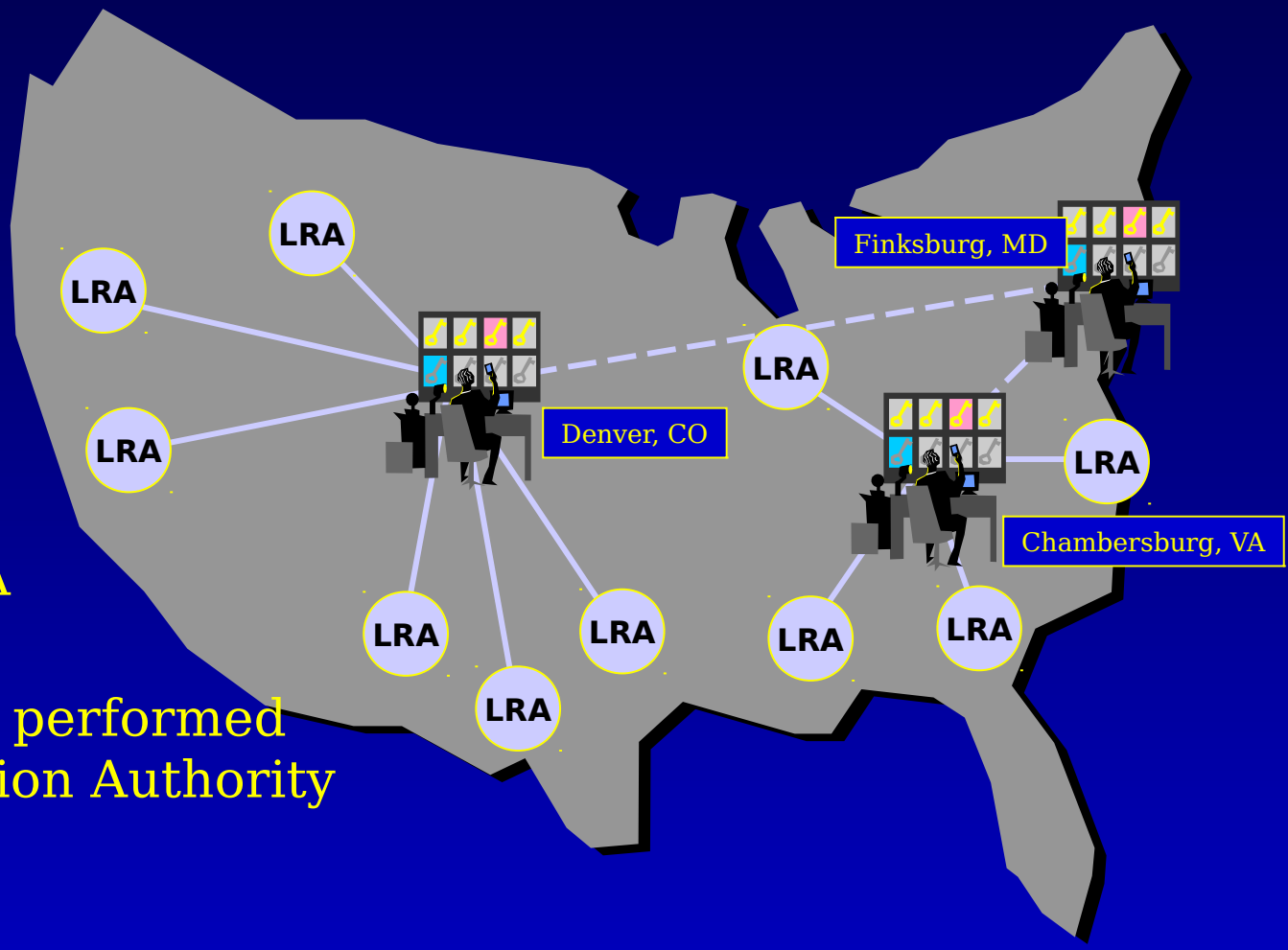
A Certifying Authority is an organization that issues public key certificates.

Where is DoD's CA?

Root CA is in Finksburg, VA (Maintained offline by DISA)

Regional CA's in Denver, CO and Chambersburg, VA

Local Registration performed by Local Registration Authority (Base-level)



How are identities bound to keys?

1) User meets with a Local Registration Authority (LRA).
   - LRA verifies the User's identity and vouches for the identity of the User with the CA.
2) A Key Pair is generated. (How this happens may vary. This is a matter of policy.)
   - The Public Key is sent to the CA, which issues a Certificate containing the User's name, Public Key and other information.
   - The Private key is stored on some hardware device (floppy disk or hardware token) and given to the user.

Review:
How do all these things fit together?

- A *Private Key* and corresponding *Public Key* form a *Key Pair*
- Public Keys are bound to identities by *Certificates*
- Certificates are created by *Certifying Authorities*
- Certificates are stored via *Directory Services*

DoD Issues

- Certificate Revocation Lists
  - Management
  - Client-side verification
- Private Key Storage
- Key Escrow
- Legacy System Applications
- Maintenance and Sustainment
- Technology Integration
  - GCCS and GCSS Frameworks

AF PKI Implementation Issues

- Requirements vs. downward directed approach
  - AF PKI PMO originally planned mass PKI registration at each AF site
  - AF PKI PMO directed to wait on requirements rather than mass roll out
  - Functional AISs have not been directed to PKI enable (AFCIC opposed to such direction)
- Required documents incomplete
  - Certificate of Net Worthiness - in process
  - Certificate to Operate - in process, but red
  - JTA-AF - in process

DoD PKI PMO Proposed Milestones

PMO* (OSD)

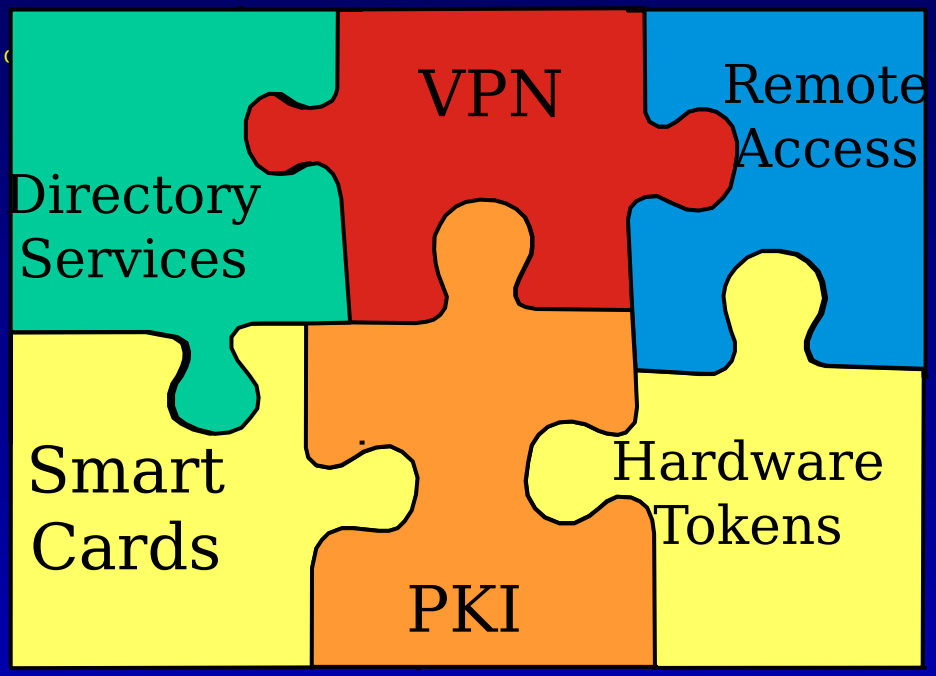
- Private web servers use PKI & SSL Jun 00 (Jun 00)
- Local Registration Authorities (LRAs) trained and in place Oct 01 (Oct 00)
- Users issued Class 3 certificates Mar 02 (Oct 01)
- Servers use client authentication Mar 02 (Oct 01)
- Sign email; encourage encrypt Mar 02 (Oct 01)
- Start transition to Class 4 certificate Oct 02 (Jan 02)
- Complete Class 4 transition ? (Dec 02)

*Proposed but not approved

Summary

- Depicted interdependencies and relationships among:

- How does this affect the Interservice (



Questions

Backup Slides

Examples

- Digital Signature
- Encryption

Definitions: Virtual Private Network

- System allowing remote access to a network through the Internet
- A virtual tunnel is created between the remote user(s) and in-house servers via encryption
- Strong authentication imperative
- Replaces or augments dial-up access via AF modem pool
- No AF standard exists

How does a PKI Digital Signature Work?

- Ralph would like to send Marlene a digitally signed message
- Assumptions:
  - Both users trust a common CA
  - Marlene has never interacted with Ralph

Ralph

Marlene

Digital Signature Example: Sender's Side

Ralph

Ralph creates a message using a PKI-
messaging program (e.g. Outlook 98).

Ralph elects to digitally sign the mess

The program creates a hash of the me

This hash is then encrypted using Ralph's Private Key.

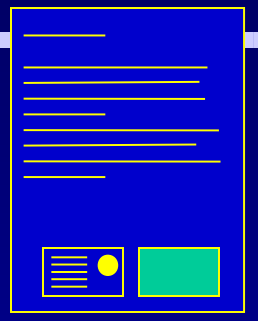
Hash?

The resulting digital signature is appe
to the message.

Ralph's Public Key Certificate is appe
to the message.

The message is sent.

Digital Signature Example: En Route



- Message is sent via conventional systems, in clear text.
- Susceptible to eavesdropping.
- If the message is changed during transit, the encrypted hash will not match the changed version.

Digital Signature Example: Recipient Side

Message appears in Marlene's inbox.

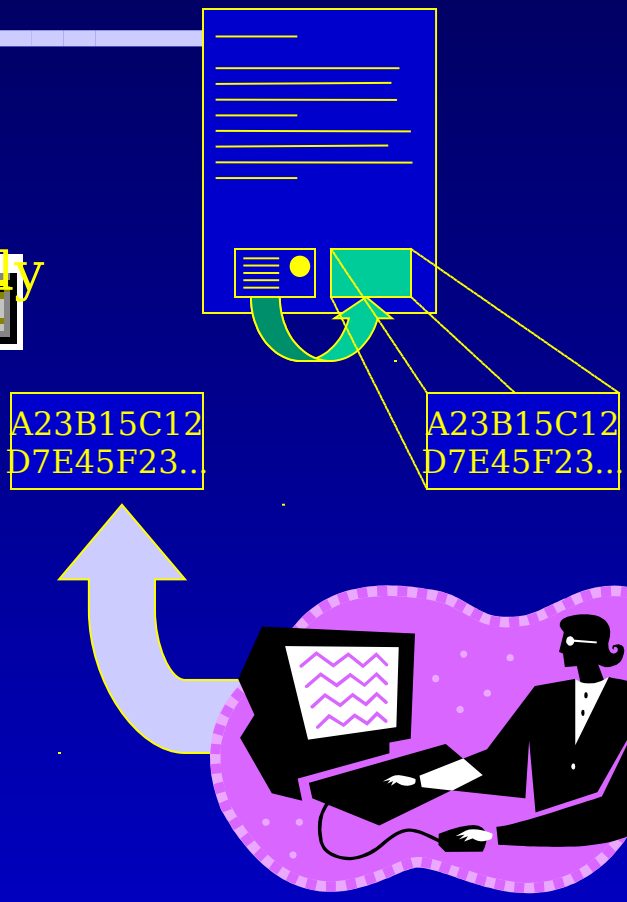
The icon associated with the message indicates that the message was digitally signed.

Marlene gets Ralph's Public Key from the CA-signed Certificate attached to the message..

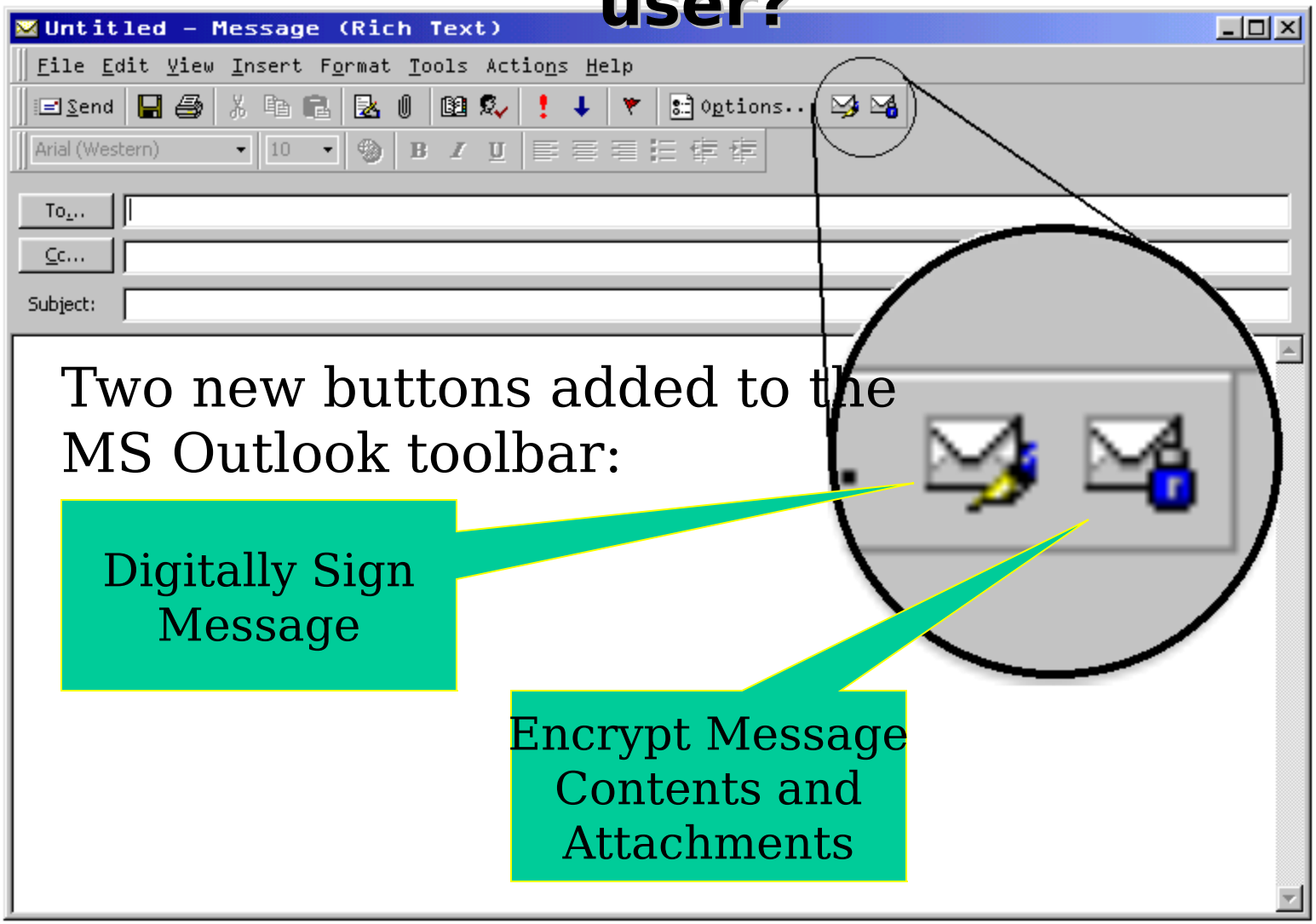
Marlene's messaging software generates a hash of the message.

It then uses Ralph's Public Key to decrypt the digital signature - yielding the hash generated on Ralph's end.

If the hashes match, the document is known to be unaltered and *Ralph's identity is validated*.



What will this look like for the typical user?



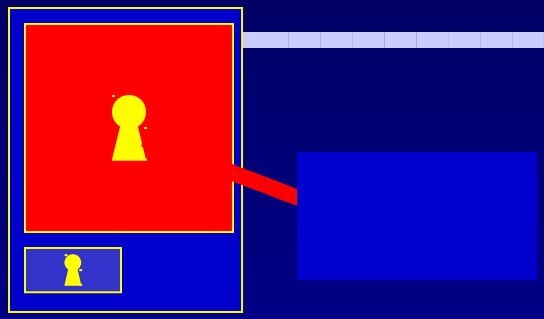
How does a PKI Encryption Work?

- Ralph would like to send Marlene an encrypted message.
- Assumptions:
  - Both users trust a common CA.
  - Ralph and Marlene have one another's Public Keys

Ralph

Marlene

Encryption Example: Sender's Side



Ralph

Ralph creates a message using a PKI-enal messaging program (e.g. Outlook 98).

Ralph elects to encrypt the message.

The program adds a digital signature to t document, as in the previous example.

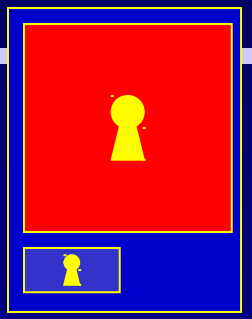
The program generates a *Session Key*.

The program encrypts the message using the Session Key.

The program encrypts the Session Key us Marlene's Public Key. The encrypted Sess Key is appended to the message.

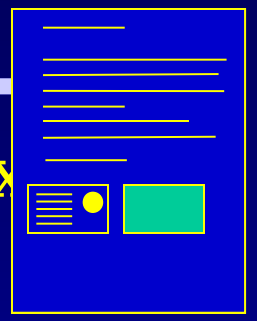
The message is sent.

Encryption Example: En Route



- Message is sent via conventional systems
- Not susceptible to eavesdropping (Denial of Service attacks still possible)

Encryption Example: Recipient Side



Message appears in Marlene's inbox

Marlene's Messaging software uses her Private Key to decrypt the Session Key.
It then uses the Session Key to decrypt the message.

Marlene uses Ralph's Public Key to verify the signature, as in the previous example.

Marlene

DoD Classes or Levels of Assurance

Class 2 - intended for applications handling informatio
low value (Unclassified, Non-Mission-Critical and of lo
monetary value) or protection of system high informat
a low to a medium risk environment.

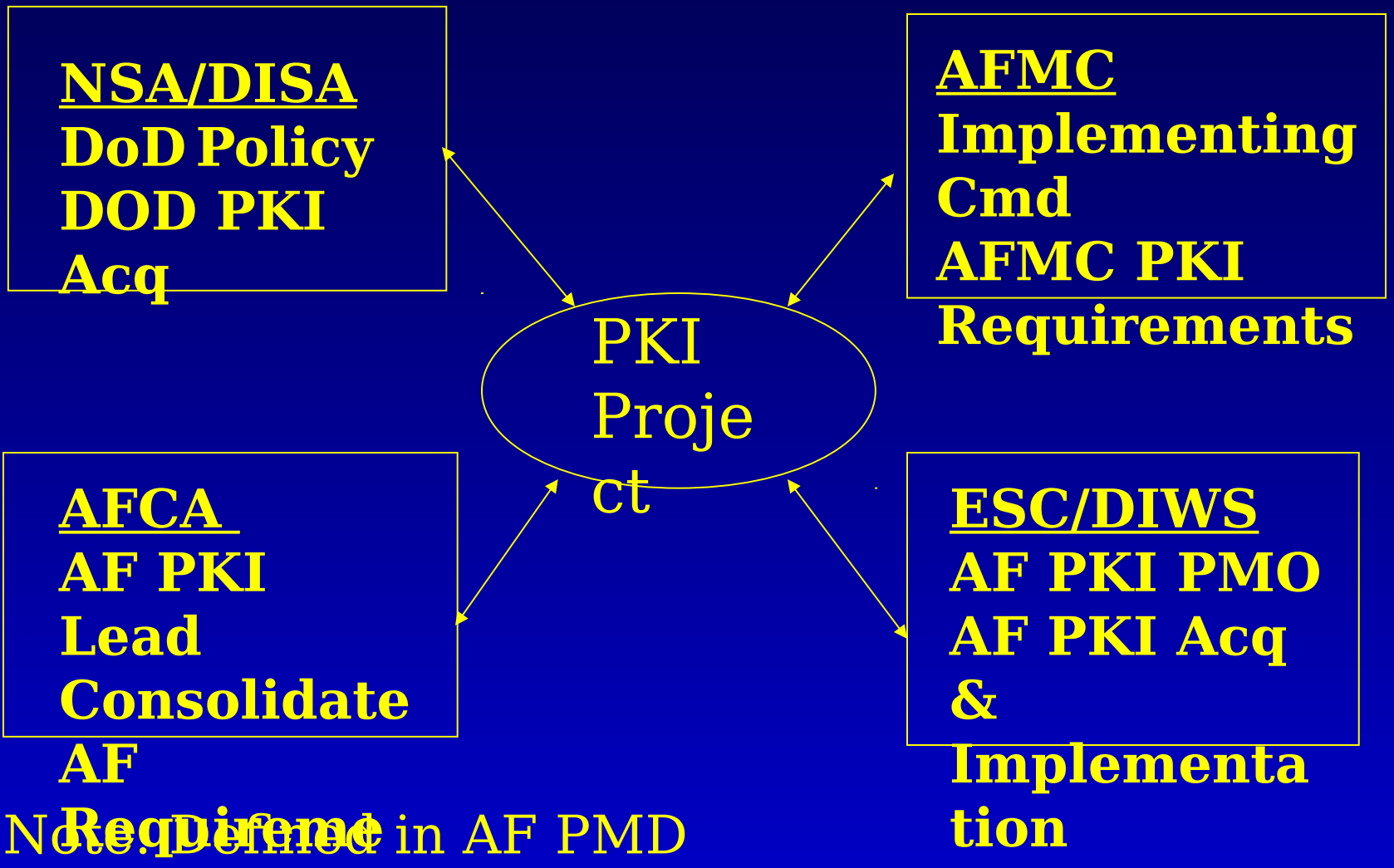
Class 3 - intended for applications handling medium v
information in a low to medium risk environment. This
assurance level is appropriate for applications that typ
require identification of an entity as a legal person, ra
merely a member of an organization.

DoD Classes or Levels of Assurance (Concluded)

Class 4 - intended for applications handling medium value information in any environment. These applicat typically require identification of an entity as a legal p rather than merely a member of an organization and a cryptographic token for protection of the private key r

Class 5 - intended for applications handling high valu information in a high-risk environment.

Coordination and Integration



PKI Summit: Security Issues

Private key distribution:

First spiral (Level 3) will use a private key stored on password-protecte

Presents serious problems for servers requiring unattended restarts cannot be “scripted.”

Some discussion of using Super Disks to increase security.

Hardware keys (Level 4), like Fortezza, will be implemented in later spir

Note: Windows 2000 does not yet support hardware authentication for l

Certificate distribution:

Estimated 700,000+ certificates required AF wide.

(66,000+ at AFMC)

Timeline: Limited start Jan 00. Formal start Jun 00. Deadline Oct 01

24 teams of 1 technical + 3 administrative to visit all installations.

Certifying Authority (CA):

Unresolved: Windows 2000 requires a Microsoft CA. Effects logon authe but not Exchange. (FIPS 140 issue)

PKI Signatures:

Non-repudiation not tested in a civil court

PKI Integration Challenges

Challenge	Areas of Impact: People	Guidance	Software	Hardware
DoD agent certificates versus non-DoD certificates (i.e., foreign nationals, contractors, family members, etc.) for e-mail	X	X	X	X
Interoperability across AF MAJCOMs and the other Services	X	X	X	X
Multiple certificate directories (i.e., replication issues due to the various types/kinds of certificates)	X	X	X	X

PKI Integration Challenges

Challenge	Areas of Impact			
	Software	Hardware	People	Guidance
Netscape versus Microsoft NT/WIN 2000 * FLIPS 140 compliance * NT good for domain level deployments, not enterprise * Synchronization of NT objects with Netscape objects	X	X		X
Compatibility issues between the COTS (Netscape/Microsoft) implementations of PKI	X	X	X	

PKI Integration Challenges (concluded)

Challenge	Areas of Impact			
	People	Guidance	Software	Hardware
Private key/certificate storage anomalies	X	X	X	X
SECURID offers a stronger authentication solution than storing it on a floppy disk.	X	X	X	X
Need to integrate SECURID with PKI	X	X	X	X
CITS/BIPS (i.e. firewall) compatibility with PKI encryption/decryption activities and information traffic coordination through proxy servers	X	X	X	X
Embedding of Private keys in scripts used for automatic recovery/backup of servers	X	X	X	X

PKI/DS Deficiencies Identified

- Directory access/email client capabilities need improvement -
  - Certificate visibility in GAL
  - Display multiple attributes (certificates)
  - Certificate Revocation List (CRL) distribution
  - Schema modifications to add certificate attribute
- Centralized key escrow
- Online Certificate Status Protocol

DS Integration Challenges

Challenge	Areas of Impact: People	Guidance	Softwa
Workstation configuration (most sites have 4/5 different configurations based on user type/requirements)	X	X	X
Common architecture across various echelons (i.e., DoD, Service, MAJCOM, etc.) and conversion from today's infrastructure to an AF common architecture	X	X	X
Netscape vs. MS WIN2000 (i.e., Dynamic vs. Static IP address management and administration*	X	X	X

DS Integration Challenges

Challenge	Areas of Impact: People	Guidance	Software	
Establish user access/account setup for each site (DoD/AF <AFCA/DMS> working groups)	X	X		
DS Naming Convention Standards, evolving from a network centric to a directory service centric solution	X	X	X	
DMS integration with WIN2000		X	X	
SATAF is evolving to single master (user) NT domains & multiple resource domains	X	X		

DS Integration Challenges (concluded)

	Areas of Impact		
Challenge	**People**	**Guidance**	**Software**
Willingness to migrate from static DNS to a dynamic DNS	X	X	
Lack of understanding of DS structure issues as they pertain to AF users getting access to corporate data (assets)	X	X	X
Message/file encryption/decryption and it's integration of anti-virus software and desktop management/administration	X		X

DNS = Directory Naming Std

MISSI is

MISSI develops standards, protocols and interfaces that define a cohesive security architecture for an evolving set of security solutions. The logical extension of NSA's MISSI efforts is a future where NSA continues to work cooperatively with industry and users to develop and field secure and interoperable COTS software for the rapidly approaching multimedia environment. In support of the DoD and its supporting agencies, MISSI provides evolutionary and affordable security solutions for meeting the security needs of a wide variety of current and emerging information systems activities.